U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Argonne NATIONAL LABORATORY

Recommendations to State Energy Officials for Cyber-Focused Energy Security Planning

May 2022

Disclaimers

- This resource is intended to inform state energy officials' cyber-focused energy security planning efforts by identifying key stakeholders to contact, questions to ask, actions to take during an incident, resources to look for, and other planning considerations.
- These recommendations are not meant to be prescriptive in nature.
- Each state will have slightly different needs based on designated authorities and responsibilities, and how they approach cybersecurity for energy infrastructure and planning purposes.

Cyber Focused Recommendations

Planning & Preparedness

1) Understand your State's Cyber Landscape

2) Establish Cyber Information Partnerships

3) Identify Cyber Response Resources

Smart Practices

1) Support Collaboration & Coordination

2) Keep Paper Copies & Contacts on Hand!

3) Participate in a Cyber Tabletop Exercise

1) Planning & Preparedness: Understand your State's Cyber Landscape

Goal: Align cyber-focused energy security planning with existing state plans where possible

- ❑ Evaluate your state's existing cybersecurity plans to determine if they:
  - Include cyber risks to the energy sector and/or critical energy infrastructure
  - Address cyber risks for operational technology (OT) systems that directly monitor or control industrial equipment (*ICS or SCADA terms may be used instead of OT*)
  - Include contacts for operators of privately owned energy infrastructure
- ❑ Identify which state entities have a role in energy cybersecurity. This typically includes public utility commissions, homeland security agencies and emergency management agency.
  - Review NASEO's Cybersecurity Pathways Guide, which examines possible SEO cyber responsibilities

2) Planning & Preparedness: Establish Cyber Information Partnerships

Goal: Gain access to cyber threat information relevant to the energy sector

- ❑ Contact your state's fusion center or intelligence partners to:
  - Identify available threat information sharing resources. Find contact information here.
  - Ask to receive security briefings focused on energy sector threats
- ❑ Work with state legislative and regulatory authorities to identify mechanisms for energy companies to share information without fear of reprisal
- ❑ Multi-State Information Sharing and Analysis Center (MS-ISAC):
  - Establish a protocol or procedure for the State Chief Information Security Officer (CISO) or Chief Information Officer (CIO) to share cyber threat information relevant to the energy sector from the MS-ISAC.
- ❑ Cybersecurity Risk Information Sharing Program (CRISP):
  - Encourage energy companies in your state to participate in bi-directional information funded by the DOE and managed by the Electricity Information and Analysis Sharing Center (E-ISAC).

3) Planning & Preparedness: Identify Cyber Response Resources

Goal: Identify resources to respond to cyberattacks on the energy sector

- ❑ Cyber assistance / mutual aid programs are available upon request to provide resources (e.g., services, personnel, equipment). The SEO should encourage partnerships with governmental and private sector cyber incident or emergency response teams.
  - **Emergency Management Assistance Compact (EMAC):** EMAC is law in all 50 states, DC, Puerto Rico, Guam, USVI and CNMI
  - **National Guard:** may have cyber units in your state or region. Identify what resources they can offer prior to or during a cyber event. Understand if a Governor's emergency declaration is required to activate state National Guard cyber forces.
  - **Electricity Subsector Coordinating Council** (ESCC)'s Cyber Mutual Assistance (CMA) Program (The ESCC CMA Program is not a government resource. States should be aware of how electric companies use their own mutual aid.)
  - **Federal partners** (FBI, CISA, DOE)
- ❑ Prepare Waivers in Advance & Know the Process to Issue
  - Cyber incidents with physical impacts may require additional measures to be taken. Review DOE's Energy Waiver Library for information on emergency regulatory relief available to support energy response and recovery efforts

1) Smart Practice: Support Collaboration and Coordination

Goal: Provide a venue for stakeholders to share unique knowledge and needs

- ❑ SEOs are encouraged to host and/or participate in other stakeholders' cyber trainings, symposiums, working groups, tabletop exercises, etc.
    - Invite both public and private sector participants from the state as well as partners from neighboring states or the region when possible.

These activities provide a venue for groups to share their unique knowledge and needs – including best practices and their approaches to preparedness and prevention, threat discovery, and incident response. They also serve to build the contacts and relationships that enable collaboration and can be crucial to successful incident response.

2) Smart Practice: Keep Paper Copies & Contacts on Hand!

Goal: Enable communication without online access

- ❑ During a cyber incident, access to digital resources, including incident response plans, emergency contact lists, etc. may not be possible
- ❑ SEOs should work with PUCs to encourage electric and ONG providers to include back-up communication options in their emergency response plans, and maintain hard copies of plans
- ❑ SEOs should maintain their own hard copy contact lists for state energy officials and keypersonnel at energy companies within their state

3) Smart Practice: Participate in a Cyber Tabletop Exercise

Goal: Improve understanding of roles, validate plans and identify gaps in exercises that test response to a cyber incident affecting energy infrastructure.

- ❑ Cyber exercises allow energy stakeholders to practice info sharing and coordination during a cyber incident and to identify planning & response gaps.
- ❑ State emergency management agencies hold annual preparedness and response exercises annually.
- ❑ Exercises such as DOE's Liberty Eclipse and NERC's GridEx include representatives from various state agencies as well as energy owners & operators, NGOs, and federal partners.

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Argonne NATIONAL LABORATORY

Understanding Your State's Cyber Landscape Questions To Ask Other State Officials

Questions to Ask State CIO, CISO, Emergency Manager, or PUC

Goal: Identify existing information sharing mechanisms, information recipients, and gaps.

1. How does [state] receive/share cyber threat intel? Is cyber threat information available to the private sector, and if so, how?
   - If unclassified information is not being made available to the private sector, the SEO should consider potential mechanisms to increase information sharing with appropriate entities
   - If SEOs are not receiving unclassified information, they should ask to be added to briefings as appropriate
   - Details that may be of interest include state participation in information sharing and analysis centers (ISACs), fusion centers, briefings, subscriptions to vendor-provided data feeds, industry and community-specific partnerships, etc.

Questions to Ask State CIO, CISO, Emergency Manager, or PUC

Goal: Identify cybersecurity resources that the state energy office can circulate widely and champion.

2. Does [state] have any cybersecurity resources (grants, training, other assistance) available to municipal or private sector organizations?
    - Since most energy infrastructure/resources are privately-owned, the intent is to identify existing state programs or federal programs that the SEO may be able to promote. (For example, Bipartisan Infrastructure Law Programs through DOE or DHS)

Questions to Ask State CIO, CISO, Emergency Manager, or PUC

Goal: Identify resources for cybersecurity incident response

3. Does [state] have cybersecurity response teams? Cybersecurity working groups?
   - These working groups are familiar with state-level cybersecurity policy, procedure, and capabilities. They can help inform energy security plans to ensure cohesiveness with other state efforts. Additional details to identify include:
     - Are these teams *active* (working together on regular basis) or only *called upon* during an incident? Is there **ICS, OT,** or energy-specific expertise on the team?
     - Do they monitor signs of compromise/breach/attacks? With whom do they share info?
       - Are there resources that may assist smaller utilities with limited cyber staff?
       - Incident response: What is the process for engaging the team? Are they only for state-level incidents, or can they be called upon for more localized incidents? Can municipal utilities request their assistance? Can commercial utilities (private industry) request their assistance?

Questions to Ask State Emergency Managers or PUC

Goal: Identify opportunities to validate energy plans / test coordination in future exercises.

4. How often does [state] exercise its incident / emergency response plan? (Exercises help evaluate emergency plans, identify gaps and inform updates)

   - Follow-up questions to consider asking:
     - Have any previous exercises dealt with cyber incidents involving the energy sector?
     - Do the exercises include partners in the private sector?
     - How are lessons learned incorporated into updates to the response plans?

Questions to Ask PUCs

Goal: Understand the cybersecurity maturity and preparation level and identify possible gaps where SEO's convening ability may be beneficial

1. What level of cybersecurity protections or plans are in place with the utilities you regulate? Have any completed and shared a cybersecurity maturity assessment? Do all of the utilities have a cyber incident response plan? What gaps or concerns do you have?
    - Review the current status of cyber preparedness, planning and investments.

2. Are there areas you think the State Energy Office may act as a convenor to host some of these cyber discussions with state and energy partners?